New Text Document.txt

12 January 1998

This paper was downloaded from the Internet.

19980114 062

MISSION NEED STATEMENT (MNS)
for
GLOBAL COMMAND AND CONTROL SYSTEM (GCCS)

May 1995

1. Defense Planning and Guidance Element

a. This Mission Need Statement (MNS) responds to the Defense Planning Guidance (DPG), FY 1996-2001, Section III, Command, Control, Communications, Computers, and Intelligence (C4I) and Space Base Systems. The following guidance is extracted from the DPG:

"Components will continue to develop a family of joint strategic command, control, communications, and intelligence systems based on an open architecture designed to support strategic and theater forces. Consistent with C4I for the Warrior initiative, focus on the interoperability as the driving requirement for joint systems. Ensure that the systems' capabilities and survivability are appropriate to both strategic and theater forces. Where appropriate, integrate efforts to improve C4I system support. Maintain a rapidly deployable communications capability to support the warfighter."

b. The stated DPG aligns with the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) memorandum concerning migrating systems to a common environment (1 November 1993, Selection of Migration Systems). Other documents that guide this effort are the Joint Chiefs of Staff C4I for the Warrior (C4IFTW) Concept; the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6721.01 (18 February 1995, Global Command and Control Management Structure); and CJCSI 6212.01, (30 July 1993, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems). It is consistent with the Command and Control Functional Analysis and Consolidation Review Panel Report

(29 October 1991). Also, it supports the concepts put forth in the following programs: the Navy's "Copernicus"; the Air Force's "Theater Battle Management/Reachback" and "Horizon Program"; and the Army's, "Early Deployment Force/Split-base Operations/Command and Control (C2) on the Move."

c. This MNS is intended to be one of several within the C4I for the Warrior Concept (C4IFTW) and defines the C4I capability that must exist from the National Command Authorities (NCA) to the CINCs; between the supported and supporting CINCs; from the supported CINC to the Commander Joint Task Force (CJTF); and from the CJTF to the component commands. This MNS states a required need for selected common functionality between the combatant commands, Services, and agencies which will allow interconnecting to the theater and task force level communications infrastructures. Requirements include information pull, collaborative planning, and teleconferencing.

2. Mission and Threat Analysis

a. **Mission Analysis.** The NCA implement command and control (C2) through a process that extends global influence over our national agencies, military forces, allies, and ultimately, over our adversaries. The process is extended through a system which provides NCA and subordinate leaders with a means to exercise their authority and direction. This process uses information to coordinate resources toward common mission objectives. It involves a continuous dynamic interaction between information, the organization, and a support system. Warfighting CINCs, subunified

commands, CJTFs, their respective Service components, and coalition forces require the ability to respond rapidly and appropriately to contingencies.

b. **Objectives**

(1) The primary objective of GCCS is to have an architecture consisting of C2 forces and elements within a highly flexible system. It must be able to collect, process, disseminate, and protect information. It will support the NCA and subordinate elements in the generation and application of national power.

(2) A requirement of unified theater and task force crisis management is to ensure that C4I systems can be configured to achieve optimum crisis response. During noncrisis operations, these forces will normally be employed in Service operations (e.g., training, peacetime engagements). The challenge facing the Department of Defense (DOD) is to integrate these existing systems into a "system of systems" to effectively meet the needs of the combatant commands, Services, agencies, and the CJTF.

(3) Commanders use information to support decision making and to extend influence over their organizations, forces, and adversaries. Information is the principal link to control execution. It impacts forces, resources, and battlespace. To prevail over adversaries, our decision and execution cycle must be consistently faster and more reliable than theirs. Therefore, the ultimate objective of national C2 is to achieve unity of effort and command dominance. Unity of effort integrates all aspects of national power and yields the full range of military force capabilities when and where required.

(4) According to "The Force Projection Cycle," (1 August 1994, Concept of Operations, Draft), in order to "fight and win decisively," the CJTF must:

· Mobilize

· Sustain

· Deploy

· Employ

· Regenerate

· Redeploy

· Train

· Maintain

The C2 systems supporting this cycle must be effective during deliberate and crisis action planning and execution. Interactive, interoperable tools (software/hardware) are required to rapidly update plans and view current operational status. Information must be univer-sally viewed, represented, and updated by the combatant commands, Services, and agencies.

(5) Joint forces must have a joint system for developing and updating time-phased force and deployment data (TPFDD) and unit movement requirements. The joint system must have the capability of supporting remote users in austere conditions and multiple joint forces. It must have capabilities for on-line transaction updates for reference files and batch file replacement. Also, it must be able to support teleconferencing and the ability to send and receive messages. Multilevel, secure, hard-copy communication capability is especially critical to the National Military Command Center (NMCC). The system must be able to transmit and deliver emergency action messages to the CJTF or the command component.

(6) The CJTF requires access to current intelligence and tactical information over a

global C4I infrastructure that can support joint and coalition missions. Intelligence information is dynamic and often affects the planning and execution phases. It is critical that it be continuously reviewed and updated.

(7) Joint forces require decision and execution cycles that are consistently faster and more reliable than the enemy's. Common software applications, communications methods, integrated databases, imagery, teleconferencing, and an open architecture are important for reducing time in the joint decision cycle.

(8) Joint and multinational force interoperability is a required long-range objective. The mid-term solution will require possible interface modifications to allow the United States (US) system to interact with our allies without compromising national security information. Any solution must address the use of space resources that are required for worldwide connectivity.

(9) Private industry is progressing toward open systems, user friendly software, and client-server architectures. The Government must leverage its automation investments by using commercial off-the-shelf software (COTS) with appropriate security. Otherwise, it will be forced to maintain outdated systems. The objective of GCCS is to take advantage of industry de facto standards and user friendly software. The software will be portable for a wide range of system architectures.

(10) Modeling and simulation systems are required to effectively plan and assess operational effectiveness and to support analytical requirements for course of action development. Rapid scenario construction for training, mission rehearsal, and after-action evaluation can be supported through the use of simulation systems.

c. **General Capabilities**. Systems will conform to standards and common software environments. GCCS will be an infosphere (information sphere) of software and hardware that will link systems together during operations. An infosphere consists of distributed global networks, computer hardware and software, space-based C2 support, and other related support systems. Five needed capabilities are:

(1) Maintenance of a Common Perception of the Crisis. This involves the requirement to maintain a consistent land, sea, air, and space operational picture across the force. Higher echelons will require less timeliness and detail. Some elements may not require all elements of the picture. Information accessible to a given command node should always be consistent with equivalent information at another node. A common perception of the crisis includes consistent information on force status and capabilities. This will include overall crisis assessment information (e.g., system vulnerabilities, target priorities, battle damage) and critical indications and warnings.

(2) Access to Planning Support Information via the Theater Infosphere. Planning support must be available on a "push" or "pull" basis as required by the CJTF. "Push" implies over-the-air updating initiated by the source and based on predetermined criteria. "Pull" implies the provision of tailored information upon specific request. A standard interface to the theater/operational infosphere must be provided to all C4I systems. It must permit access in either the "push" or "pull" mode to multimedia information on:

· Intelligence and imagery data bases and analysis

· Environmental, oceanographic, topographic data bases and analysis

· Deployment analysis, requirements, generation, transportation data bases, and monitoring systems

· Logistics analysis, requirements generation, medical, and personnel data bases/systems

· Non-Defense and Non-US data bases as required to support selected missions

· Analysis, news broadcasts, teleconferencing simulation centers, and gaming centers

(3) Collaborative Access to a Common Operational Plan. The theater-level joint operation planning and execution community (JPEC) procedures require collaboration between the combatant commands, supported commanders, agencies, Service components, the CJTF, and the subunified commander. This requirement includes the development, refinement, and evaluation of a CINC's assessment and joint operational plans. Improvement is required for collaborative development of the plan and to refine, coordinate, and prioritize/deconflict resources and schedules. The specific processes that must be supported are:

· Courses of action (COA) development

· Forces and task refinement

· Employment analysis

· Specialized employment analysis (e.g., employment of special capabilities that may not currently be in the theater)

· Deployment/transportation analysis

· Sustainment analysis

· On-line refinement teleconferencing

· Remote briefing

· Tailored plan dissemination

The requirements of this process can be identified with the concept of a series of joint "anchor desks." These are information/planning support facilities accessible to the CJTF via standard protocols. Their primary function is to interface mission or functional specific, rear-echelon support facilities (e.g., intelligence, weather, planning/analysis centers) to the infosphere. This element, added as a front-end to existing systems and centers, provides the warfighter with supporting information and "reach-back" access to specialized analysts and planners.

(4) Visibility of Plan Execution Status. At the tactical level, commanders must build a campaign plan from the operational directives given by the CINC. They must be able to access selected resource information from the task force or subunified command components in order to perform resource allocation and task planning/scheduling. Collaborative tactical plan development requires visibility of overall target/task priorities, component battle plans (i.e., air, land, sea, space), operational constraints, and the ability to deconflict these against the CJTF's campaign plan. This requires a common target/task representation across systems. All operational components must have the ability to readily monitor critical tasks and resource status. They must be able to monitor critical task execution of external resources (e.g., transportation, medical, logistics support). Theater-level providers must maintain a controlled degree of visibility into critical expenditures, causalities, weather conditions, and information to predict shortfalls.

(5) Adaptive Control of Communications and Information Centers for Surge, Degraded Users, and Incremental Deployment. The C4I infosphere must be able to adapt to the availability and accessibility of its supported information. A highly capable unit, such as a Navy command ship or an Army Corps command complex might be able to access the infosphere via wideband SHF and commercial wideband services. A small joint special operations task force might be capable of only limited bandwidth UHF communications. Usually, deployment/relocation of major information centers is incremental. An airborne or small advance party is deployed initially, followed by augmentation and communications systems.

d. **Threat Analysis**. Peacetime threats include the following:

· Foreign intelligence collection

· Intercept/analysis of communications and networks

· Attacks against automated systems and information

· Spoofing

Threats during crisis conflict include the following:

· Physical or electronic attack

· Destruction by national or terrorist entities

· Attempts to capture infosphere elements

· Use of directed energy devices

· Employment of jamming and deception

· Information warfare

Other crisis threats include the environment (e.g., earthquakes, volcanoes). These can cause destruction, interruptions, and additional stresses on the system. All of them may necessitate collaborative planning to transport people, equipment, and supplies. Regional conflicts are increasing with the proliferation of weapons of mass destruction. Also, the possible use of nuclear, chemical, and biological weapons must be a factor in crisis planning. Added threats in the event of global war could include nuclear blast, radiation, scintillation, high-altitude electromagnetic pulse (HEMP), antisatellite weapons, and high-altitude nuclear bursts. This MNS emphasizes threats that occur during conventional crises.

e. Mission Deficiencies

(1) A C4I Interoperability Tiger Team (5 June 1992, C4I Interoperability Tiger Team Memorandum) was established by the Joint Staff's Director for C4 to determine joint command, control, and information interoperability requirements. The Tiger Team determined that existing systems providing C2 capability to the NCA do not provide end-to-end automation. Many of them are noninteroperable and are not responsive to the user's needs. The Tiger Team identified the following required C4I system functionalities:

· Crisis planning

· Force employment

· Force status

· Logistics

· Air operations

· Fire support

· Intelligence

· Personnel

· Position

· Narrative information

· The integration of all the above functionalities

GCCS must integrate new procedures and create interoperable functionality to enhance information gathering. Existing C2 systems (primarily the Worldwide Military Command and Control System (WWMCCS)) are not capable of being modified to meet these requirements.

(2) WWMCCS is dependent on a proprietary mainframe environment. Information cannot be easily entered or accessed by users, and the software cannot be quickly modified to accommodate changing mission requirements. Operational flexibility and adaptability are limited, since most of the information and software are stored on the mainframe. The system architecture is unresponsive, inflexible, and expensive to maintain.

(3) Service, combatant command, and agency systems' capabilities differ radically (e.g., ground maneuver and fire support versus air operations tasking). There is no single system that currently comes close to satisfying even a majority of the aggregate information and functional requirements. Migration of systems to a common environment is the preferred method of development for required common functionalities. Software that is not aligned with the baseline common operating environment (COE) standards will require conversion.

(4) The combatant commands, Services, and agencies are currently protecting operational planning data in a Top Secret mainframe environment. The need for information to be in a multilevel security environment has been identified as a critical requirement. It is costly and cumbersome to protect all information as if it were classified Top Secret. A temporary solution is being initiated that will process information on a central mainframe for each combatant command, Service, and agency that has a Top Secret requirement. The next phase will be a multilevel security (MLS) environment that will be fielded to each combatant command, Service, and agency. The MLS solution will process information on a client-server environment. It will be a composite of hardware and software products. [Note: Until MLS is available, operationally suitable and affordable, GCCS will operate in the system-high SECRET mode.]

3. Nonmateriel Alternatives. No doctrinal, operational concept, organizational, or training changes will correct the problems with the existing C2 systems. Only materiel solutions will increase the ability to achieve C4I interoperability.

4. Potential Materiel Alternatives. Presently there are no materiel alternatives that will fulfill the stated requirements in this MNS. Combatant command, Service, and agency requirements and system capabilities differ radically. No single system is currently addressing the entire spectrum of functional requirements. Existing combatant command, Service, and agency architectures will serve as a foundation from which C4I system requirements and capabilities will evolve. The desired environment, GCCS, will have the capability to utilize leading-edge technologies as they become available. The effort would provide a common set of infosphere software to provide network interfaces, file maintenance, and operator windows for crisis planning and execution. Service, combatant command, and agency unique functions would be unaffected.

5. Constraints. The requirements and needs prescribed in this MNS must be achieved through an orderly migration from existing systems to the GCCS environment. The first phase will provide the force commander with a fused battlespace picture. Phase two consists of the "Best of Breed" process and will be completed when all required WWMCCS functionalities (e.g., Joint Operation Planning and Execution System (JOPES)) have successfully migrated to GCCS. WWMCCS and the existing legacy systems will be turned off at the end of phase two, with the concurrence of the users. During phase three, long-term goals will be reached by improving interoperability, and implementation of standards (e.g., communications resources, common information sources, security policies, procedures, and training). This will include robust tools to allow the user to build applications in a common C2 environment. Other constraints to consider are:

a. **Logistics**. Theater/task force crisis management capability must use existing systems as much as possible.

b. **Transportation**. Transportable C4I elements should be compatible with the provisions specified in DOD Directive 4500.32-R, Military Standard Transportation and Movement Procedures. Transportability and downsizing of C4I packages are critical to rapid deployment of an initial crisis capability. Also, important is the ability of elements to operate in-flight while the CJTF/JTF components are en route to a crisis.

c. **Mapping, Charting, and Geodesy**. Products of this community must be standardized and electronically transportable across the infosphere.

d. **Manpower, Personnel, and Training**. GCCS manpower must make the greatest possible use of existing resources and avoid the creation of systems that require additional manning. Training must be integrated into the existing DOD training infrastructure.

e. **Command, Control, Communications, and Intelligence (C4I)**. It must be possible for Service components to transition between combatant command and subunified commander areas of responsibility without changing equipment or procedures. Forces must be able to participate in single Service operations using the same infrastructure. Also, tactical systems have limited bandwidth which constrains the amount of data that can be transferred. They will have to share the available bandwidth with other uses such as voice and teleconferencing.

f. **Security**. Interfaces to coalition and non-US civilian activities often are required in crisis operations. Security and security assistance policies must be applied to the design of C4I interfaces and access. Common computer security practices must be utilized in the development and operation of GCCS. This should include the requirement for audit trails and password protection. The security for GCCS will be administered in accordance with the following regulations and instructions:

· DOD Regulation 5200.1, DOD Information Security Program

· DOD 5200.2, DOD Personnel Security Program

· DOD 5200.28, Security Requirements for Automated Information Systems

· DOD C-5200.5, Communications Security

g. **Standardization/Interoperability**. GCCS will conform to the DOD Technical Architecture Framework for Information Management (TAFIM). This includes the standards that are required for communications. Conformance to open systems standards will be used as a basis for the migration of C4I systems to the GCCS environment. Coalition interfaces must conform to agreements with NATO and other allies.

h. **Energy**. Systems will be compatible with available energy sources (especially tactical equipment) and will minimize energy consumption.

i. **Survivability**. Survivability features must be consistent with the survivability of the interfacing, supporting, and supported systems. In low-threat operations, commercial communications may be integrated into the system.

6. *Joint Potential Designator.* GCCS will be considered a joint program. Migration software will be submitted to the Defense Information System Agency (DISA) by executive agents (Services, combatant commands, or agencies). The software that is selected will be migrated into the GCCS environment, which may require some software engineering by DISA and the executive agent. The engineering funds for the initial COE and other designated joint software will be primarily funded by DISA and the Joint Staff. The executive agents or designated lead developers (Government) will

then assume the resource (monetary and other) responsibility of version or
maintenance changes. DISA will act as the project manager for technical aspects of
GCCS. The Joint Staff (J3) will assume ownership of GCCS and will provide policy and
guidance. The Joint Staff (J6) will provide the technical guidance for the
life-cycle of the project.

Last updated: 10/11/95